



8

PATENT**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Aviad KIPNIS, et al.

Serial No.: 09/552,115

Group No.:

Filed: April 19, 2000

Examiner:

For: PUBLIC KEY SIGNATURE METHODS AND SYSTEMS

Attorney Docket No.: U 013188-5

Assistant Commissioner for Patents
Washington, D.C. 20231DECLARATION UNDER 37 C.F.R. ' 1.132

I, JACQUES PATARIN, do hereby declare as follows:

I am a citizen of France, and my home address is 82 bis
avenue de Paris, 78000 Versailles, France.I am a co-inventor of U.S. Patent Application No.
09/552,115 mentioned above.

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8a)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING☒ deposited with the United States Postal Service
with sufficient postage as first class mail in an envelope
addressed to the Commissioner of Patents and Trademarks,
Washington, D.C. 20231Date: JULY 12, 2001**FACSIMILE**☐ transmitted by facsimile to the Patent and
Trademark Office

Signature

JULIAN H. COHEN

(type or print name of person certifying)

I am currently an employee of Bull CP8 (hereinafter "Bull") of France which is an assignee of the U.S. Patent Application No. 09/552,115 together with NDS Ltd. of the U.K. I have been employed by Bull for the past 10 years, and I am currently the Head of Cryptographic Department in the Personal Transaction Systems Division, a position I have held since 1991.

In September 1997, I gave one and only one presentation at the Dagstuhl Workshop on Cryptography (hereinafter "the presentation") in which I described an algorithm for signatures that I named "Oil and Vinegar". The presentation was entitled "The oil and vinegar algorithm for signatures" and it included three transparencies, copies of which were given to attendees of the presentation.

The copy of the document identified as "The Oil and Vinegar Scheme" in a Supplemental Information Disclosure Citation mailed on August 28, 2000 for the U.S. Patent Application No. 09/552,115 is a true copy of the three transparencies of the presentation.

At page 2, line 19 (as numbered) of the specification of the U.S. Patent Application No. 09/552,115, there is mentioned for incorporation by reference an "article titled 'The Oil and Vinegar Signature Scheme' presented at the Dagstuhl Workshop on Cryptography in September 1997". Further in the specification of the U.S. Patent Application No. 09/552,115, at page 26, item 9 is mentioned as, "J. Patarin, The Oil and Vinegar Signature Scheme, presented at the Dagstuhl Workshop on Cryptography, September 1997 (transparencies)".

The latter confirms that the publications titled "The Oil and Vinegar Signature Scheme" in the Supplemental Information Disclosure Statement and the specification of the U.S. Patent Application No. 09/552,115 fully correspond to the transparencies of the presentation.

The identification details "Personal Transaction Systems

Division" and "© Bull CP8 - FLIP198.PPT/J. PATARIN-L.GOUBIN" at the bottom of each transparency of the presentation only define the cryptographic entity of Bull CP8 at which the presentation was prepared, such entity including JACQUES PATARIN and LOUIS GOUBIN. The mentioning of L. GOUBIN at the bottom of each transparency is not meant in any way whatsoever to indicate that L. GOUBIN was an author of the presentation. I was the sole author of the presentation.

All statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such wilful false statements may jeopardize the validity of the application or any patents issuing thereon.

Signed



Name Jacques Patarin

Date: 11. 06. 01